COOLEY LLP
MICHAEL A. ATTANASIO (151529)
(mattanasio@cooley.com)
BENEDICT Y. HUR (224018)
(bhur@cooley.com)
SIMONA AGNOLUCCI (246943)
(sagnolucci@cooley.com)
EDUARDO E. SANTACANA (281668)
(esantacana@cooley.com)
JONATHAN PATCHEN (237346)
(jpatchen@cooley.com)
ARGEMIRA FLOREZ (331153)
(aflorez@cooley.com)
NAIARA TOKER (346145)
(ntoker@cooley.com)
HARRIS MATEEN (335593)
(hmateen@cooley.com)
THILINI CHANDRASEKERA (333672)
(tchandrasekera@cooley.com)
ISABELLA MCKINLEY CORBO (346226)
(icorbo@cooley.com)
CHELSEA HU (357212)
(chu@cooley.com)
MICHAEL B. MORIZONO (359395)
(mmorizono@cooley.com)
3 Embarcadero Center, 20th Floor
San Francisco, CA 94111-4004
Telephone: (415) 693-2000
Facsimile: (415) 693-2222
Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ANIBAL RODRIGUEZ, et al. individually and on behalf of all others similarly situated,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Case No. 3:20-CV-04688-RS

GOOGLE LLC'S MOTION TO DECERTIFY OR MODIFY THE CLASS

Dept: 3, 17th Fl.
Judge: Hon. Richard Seeborg

Date Action Filed: July 14, 2020

Trial Date: August 18, 2025

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

Other Authorities

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

Please take notice that pursuant to the schedule established in Docket 694, Defendant Google LLC hereby moves this Court, pursuant to Federal Rule of Civil Procedure 23(c)(1)(C), for an order decertifying or modifying the certified classes in this action.

The Motion is based on this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the pleadings and other papers filed, any oral argument, the evidence and testimony presented at trial, and any other such matters that the Court may consider.

STATEMENT OF ISSUES TO BE DECIDED

1. Should the plaintiff class be decertified as to, or amended so as to exclude, the invasion of privacy and intrusion upon seclusion claims (the "Privacy Claims")?
2. Should the Court vacate the jury verdict as to the Privacy Claims?

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The jury trial in this case confirms why privacy claims are ill-suited for class-wide resolution. Every element of the Privacy Claims advanced by Plaintiffs calls for individual—not common—inquiry. Plaintiffs failed to provide class-wide, common evidence that each class member actually maintained a reasonable expectation of privacy. Worse, the class representatives' testimony confirmed that offensiveness of the alleged intrusion cannot—and could not—be proven on a class basis. In short, trial demonstrated that the Privacy Claims that Plaintiffs brought to trial should not have been certified. And because "[r]ule 23(c)(1)(C) requires courts to reassess class rulings as the case develops and to ensure continued compliance with Rule 23's requirements," *Amara v. Cigna Corp.*, 775 F.3d 510, 520 (2d Cir. 2014) (cleaned up), the fact that the Court certified this action nearly two years ago does not insulate it from decertification when Rule 23 is no longer satisfied.

Class treatment of Plaintiffs' Privacy Claims is improper. The class should be decertified as to those claims and the resultant jury verdict vacated.

II. LEGAL STANDARDS

A. Decertification Standard

Federal Rule of Civil Procedure 23(c)(1)(C) provides that "[a]n order that grants or denies class certification may be altered or amended before final judgment." "[A] district court's order denying or granting class status is inherently tentative." *Coopers & Lybrand v. Livesay*, 437 U.S. 463, 469 n.11 (1978). As such, "[d]istrict courts have a responsibility to review continually 'the appropriateness of a certified class in light of developments subsequent to class certification.'" *Abante Rooter & Plumbing, Inc. v. Alarm.com, Inc.*, No. 15-cv-06314-YGR, 2018 WL 558844, at *2 (N.D. Cal. Jan. 25, 2018) (quoting *Schilling v. TransCor Am., LLC*, No. C 08-941 SI, 2012 WL 4859020, at *1 (N.D. Cal. Oct. 11, 2012)); *Amara*, 775 F.3d at 520 ("Rule 23(c)(1)(C) requires courts to reassess class rulings as the case develops and to ensure continued compliance with Rule 23's requirements" (cleaned up)); *see also Kuehner v. Heckler*, 778 F.2d 152, 163 (3d Cir. 1985); *Richardson v. Byrd*, 709 F.2d 1016, 1019 (5th Cir. 1983) ("Under Rule 23

the district court is charged with the duty of monitoring its class decisions in light of the evidentiary development of the case. The district judge must define, redefine, subclass, and decertify as appropriate in response to the progression of the case from assertion to facts."). Class certification is not dispensed in gross; it is granted or denied on a claim-by-claim (or issue-by-issue) basis. *See* Fed. R. Civ. Proc. 23(c)(1)(B). The party seeking to maintain class certification bears the burden of demonstrating that the Rule 23 requirements are satisfied, even on a motion to decertify. *See Marlo v. United Parcel Serv., Inc.*, 639 F.3d 942, 947 (9th Cir. 2011).

B. Relevant Certification Standards

To maintain class certification, plaintiffs must demonstrate that each of the four requirements of Rule 23(a) are met and one or more of the Rule 23(b) criteria are satisfied. Relevant to this motion, commonality under Rule 23(a)(2) requires the existence of at least one common question of law or fact. While plaintiffs need only identify one common question, it must be a question that is central to the litigation and one that can (and will) provide class-wide answers. *See generally Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338 (2011).

Rule 23(b)(3) requires that, for a class seeking damages, "questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods" of adjudication. Rule 23(b)(3)'s predominance requirement "imposes stringent requirements for certification that in practice exclude most claims." *Am. Express Co. v. Italian Colors Rest.*, 570 U.S. 228, 234 (2013). To satisfy it, "plaintiffs must establish that essential elements of the cause of action . . . are capable of being established through a common body of evidence, applicable to the whole class." *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 666 (9th Cir. 2022) (cleaned up).

For a case to be certified as a 23(b)(2) class action, it must comply with the four requirements of Rule 23(a) and meet the two criteria specified in Rule 23(b)(2) itself: the party opposing the class must have "acted or refused to act on grounds generally applicable to the class," and the plaintiffs must be seeking "final injunctive relief or corresponding declaratory relief" that is appropriate "with respect to the class as a whole." *Small v. Allianz Life Ins. Co. of N. Am.*, 122 F.4th 1182, 1201 (9th Cir. 2024) (reversing district court's grant of class certification under Rule

23(b)(2) where "neither an injunction forcing specific performance, nor the district court's declaration constitute 'indivisible' relief that 'benefits all its members at once'").

III. ARGUMENT

A. Class Treatment Is Inappropriate For Plaintiffs' Privacy Claims Because There Are No Common Issues As To Whether An Intrusion Was "Highly Offensive"

At class certification, the Court was provisionally satisfied that class treatment was appropriate for all three of Plaintiffs' claims. Dkt. 352 at 1, 18. Now, after a two-week jury trial and Plaintiffs' full disclosure of the evidence behind their claims, it is clear that class treatment of Plaintiffs' Privacy Claims is improper under Rule 23 and cannot be maintained.

Plaintiffs' Privacy Claims against Google are (1) invasion of privacy under the California Constitution and (2) intrusion upon seclusion. While the claims are technically distinct, they consist of similar elements. "The inquiry under either is whether (1) there exists a reasonable expectation of privacy, and (2) whether the intrusion was highly offensive." Dkt. 445 at 9 (cleaned up); *see also* Dkt. 352 at 8, 10. As explained below, trial confirmed there are no common questions that can be resolved by class-wide proof.[1] Rule 23(a)(2) is not satisfied. Even if there were some such questions, it is clear that individual issues predominate—precluding certification. Because of the volume of different third-party apps, the varying types of data they collect, and the varied types of users of each app, individualized issues predominate in analyzing whether the class as a whole had any reasonable expectation of privacy.

To prevail on their Privacy Claims, Plaintiffs must prove that Google's conduct was highly offensive. *See Williams v. DDR Media, LLC*, No. 22-cv-03789-SI, 2023 WL 5352896, at *5-6 (N.D. Cal. Aug. 18, 2023). Conduct is "highly offensive" if it is an "egregious breach of social

[1] Google hereby preserves its prior arguments challenging class certification with respect to each of the elements of all of Plaintiffs' Privacy Claims. *See, e.g.,* Dkts. 323, 662. In particular, Google expressly preserves the argument that whether each class member actually maintained a reasonable expectation of privacy is not susceptible to class-wide, common proof. Dkt. 662 at 12 n.3 (citing *Hart v. TWC Prod. & Tech. LLC*, No. 20-cv-03842-JST, 2023 WL 3568078, at *9 (N.D. Cal. Mar. 30, 2023)). Notably, Plaintiffs put forth no evidence at trial of such class-wide expectation. In this motion, Google focuses on the affirmative evidence presented by Plaintiffs at trial that unambiguously shows the lack of commonality as to the "highly offensive" elements of the Privacy Claims.

norms" or an "intrusion [] in a manner highly offensive to a reasonable person." *See id*. (citations omitted). The jury was instructed that "highly offensive conduct" consisted of conduct that was "a shocking or outrageous breach of social norms regarding online data." Dkt. 666 at 19, 21.

The type of data that is collected is a factor that courts consider in determining whether a defendant's collection or use of user data is "highly offensive." In *McCoy v. Alphabet, Inc.*, the court dismissed the plaintiff's privacy tort claims, holding that the defendant's collection of data from third-party apps was not "highly offensive." No. 20-cv-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021). In *McCoy,* the defendant collected "confidential and sensitive data," including how long the plaintiffs' and class members' used and had open certain apps. *Id*. The court noted that "no other types of data" were alleged to be collected, and since the app activity data "was not tied to any personally identifiable information, was anonymized, and was aggregated," the collection did not rise "to the requisite level of an egregious breach of social norms[.]" *Id*. "Courts in this district have held that data collection and disclosure to third parties that is 'routine commercial behavior' is not a 'highly offensive' intrusion of privacy." *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1090 (N.D. Cal. 2022); *In re iPhone Application Litig*., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (collection of "unique device identifier number, personal data, and geolocation information" did not rise to an egregious breach of social norms).

In order to overcome their heavy burden to demonstrate offensiveness on a class-wide basis, Plaintiffs offered a new theory of offensiveness at trial. Plaintiff Rodriguez explained that Google's conduct was highly offensive not because Google Analytics collected data from individual apps, but rather because he (incorrectly) believed that Google then took the data it received from individual apps and put "pieces of [the] puzzle" together. Trial Tr. Aug. 25 (Rodriguez) at 811:7-17. For example, on cross-examination, Plaintiff Rodriguez admitted that he was okay providing Google with the Analytics data collected by the Target app and that his privacy objection was to Google compiling all the sWAA-off data from all the apps on his phone. *Id*. at 812:24-813:24, 841:11-24, 842:1-843:21 ("I don't think it was a big deal"), 856:3-11.

Central to Rodriguez's new theory of offensiveness was the nature of the "puzzle pieces" (app data) and what was done with those puzzle pieces. But not all apps collect the same data, have

the same types of users, or deal with the same subject matter. If the offensiveness of the conduct depends on the effect of "putting the puzzle pieces together," the suite of apps (or even a single app) that a class member installed is highly relevant to that inquiry and not suitable for resolution on a class-wide basis. Plaintiff Rodriguez's testimony bears this out:

> **Q**: Did you ever use the **NightOwl Companion** app while you had sWAA off?
>
> **A**: Yes.
>
> **Q**: Do you consider your sleep apnea a private and personal matter?
>
> **A**: Definitely it is.
>
> **Q**: Did you ever use the **MIPC camera** app while sWAA was off?
>
> **A**: Yes. . . . It connects to my cameras in my home.
>
> **Q**: Do you consider what you do for home security a private and personal matter?
>
> **A**: Oh, yeah, definitely.
>
> **Q**: Did you ever use the **Career Karma** app while sWAA was off?
>
> **A**: Yes.
>
> …
>
> **Q**: Do you consider whether you're looking for a new job something that's private and personal to you?
>
> **A**: Yes.
>
> …
>
> **Q**: You had no problem with the **Target** app sharing your data with Google Analytics, Adobe Analytics, or Crazy Egg; right?
>
> **A**: If -- if -- understanding how -- how I see things and what I learned, I don't think it was a big deal.
>
> **Q**: Not a big deal?
>
> **A**: Not with -- not sharing my Target information, my Target activity, with the analytics company. I don't think that's an issue.
>
> …
>
> **Q**: But you allowed **your son** to use his Android phone after you filed this complaint the same way he had used it before; right?
>
> . . .

> **A**: Right. He's very young. They're not using any apps like I am. They really just used it for playing games and watching videos and stuff like that. . . . . I mean, right now I would say at that time if there's any data being collected, it's a five-year-old and a ten-year-old at the time. And, again, they're not using the phone the same way as I would where you can kind of put the pieces of the puzzle together and know who I am. I think you would say it's a five-year-old and a ten-year-old, and I don't think there's much information that you can actually gather from that. It's just kids playing on a phone. It's not using apps like an adult uses an app.

Trial Tr. Aug. 25 (Rodriguez) at 812:23-813:21, 843:12-19, 856:3-5, 856:8-858:4 (emphasis added). Plaintiffs' own testimony confirms that the ***nature*** of the app, and the ***nature*** of the data collected, and the ***nature*** of the user each bear on the reasonableness of any expectation of privacy. Collection of data from certain apps may justify a finding of highly offensive conduct, but others do not. And "putting the puzzle pieces together" for some users like Rodriguez—who had apps that track his sleep and career goals—could be highly offensive while doing so for users who only use anodyne gaming apps (like his son) is not. These admissions confirm exactly why proof of offensiveness cannot be proven class-wide, because the volume of third-party apps and the type of data they collect significantly impacts the analysis, creating a highly individualized inquiry. *See Peterson v. Aaron's, Inc.*, No. 1:14-CV-1919-TWT, 2017 WL 364094, at *8-9 (N.D. Ga. Jan. 25, 2017) (holding that whether an offensive invasion occurred is determined by the "particular circumstances of each class member" and what expectation of privacy they may have had based on the context); *Murray v. Fin. Visions, Inc.*, No. CV-07-2578-PHX-FJM, 2008 WL 4850328, at *5 (D. Ariz. Nov. 7, 2008) (reasoning that the offensiveness of forwarding putative class members' emails to another party turned on the content of each email).

Given this new theory of offensiveness, the terms of service of each individual app also become highly relevant to whether Google's conduct could be offensive. This presents highly individualized issues. It is undisputed that Google required third-party apps that used GA4F to obtain consent from its users. Users sign up or download the apps directly from third parties, without any contact from Google. Because the theory of offensiveness Plaintiffs offered at trial depended in part on the specific apps that are downloaded, the representations that the third-party apps made to those users is relevant to offensiveness. Mr. Rodriguez's testimony regarding one app—his Target app—proves the point. *See* Trial Tr. Aug. 25 (Rodriguez) at 839:9-17 (admitting

that as part of his deal with Target, he was okay with Target having analytics data), 841:11-22 (admitting that he agreed "to the use of multiple analytic services" when he read and agreed to Target's privacy policy, "includ[ing] Google Analytics"). Of course, if third-party apps made Google's role clear, that would reduce—if not outright preclude—class members from having an objectively reasonable expectation of privacy, much less be the type of "highly offensive conduct" that constitutes "a shocking or outrageous breach of social norms regarding online data." And the number of apps a user downloaded is equally relevant to the issue. *See* Trial Tr. Aug. 20 (Santiago) at 519:5-8 (acknowledging that each of the 42 apps Plaintiff Santiago downloaded had their own terms of service and privacy policies). One can easily imagine Google cross-examining a class member to explore how offensive the conduct could be when that user had downloaded scores of apps, each of which disclosed Google's role, after turning off sWAA (or having it off without even knowing it). This inquiry requires individualized proof as to the disclosures from each third-party app that used GA4F during the class period to identify what their disclosures represented to users and then mapping those disclosures to each class members. That is the antithesis of common proof.

Moreover, whether Google's conduct could be highly offensive also turned on whether a plaintiff had already consented to allowing other SDKs to collect the same data. The evidence showed each app uses—on average—four analytics SDKs. Trial Tr. Aug. 26 (Ganem) at 1145:18-24. Which suite of SDKs each third-party app employs will similarly impact the offensiveness of Google's conduct. What data is collected by those other SDKs? Do those other SDKs "put the puzzle pieces together" as Plaintiff Rodriguez falsely claimed Google does? *See* Trial Tr. Aug. 26 (Ganem) at 1130:16-1132:9, 1134:5-1135:15, 1136:25-1137:15; Trial Tr. Aug. 29 (Black) at 1722:1-24. Facebook does assemble the pieces, and Adobe has no sWAA-off button similar to Google. Trial Tr. Aug. 27 (Ganem) at 1260:23-1261:18, 1262:23-1263:17, 1267:9-15, 1268:9-22. Both Plaintiff Santiago and Rodriguez had the Facebook app and Mr. Rodriguez consented to Target providing his Target-app data with Adobe and an analytics provider so small that Mr. Ganem hadn't heard of it: CrazyEgg. Plaintiffs' Demonstratives at 1, 3; Trial Tr. Aug. 25 (Rodriguez) at 841:11-842:2l; Trial Tr. Aug. 27 (Ganem) at 1267:16-18. Indeed, the analytics SDKs implicated additional privacy issues, such as what entity ultimately controls the data and how it is used. *See*

Trial Tr. Aug. 27 (Ganem) at 1260:3-14 (explaining that Facebook owned the app data from its analytics platform whereas the app (and not Google) owns the sWAA-off Google Analytics data and how it is used). Google's conduct is far from "highly offensive" if class members—like Mr. Rodriguez—consent to similar (if not even more invasive) data collection from competitive analytics platforms. It is, as Mr. Rodriguez testified, not "a big deal." Trial Tr. Aug. 25 (Rodriguez) at 843:12-21.

Finally, because offensiveness turns on *the type* of data Google collects, this then turns on what type of data third-party apps authorized to be collected. *See Hammerling*, 615 F. Supp. 3d at 1091; *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063. To establish this, Plaintiffs needed to present sufficient evidence to identify the type of data each third-party app collected. Not only did Plaintiffs fail to do so, but doing so would present highly individualized analyses for each of the million-plus apps that use GA4F.

B. Additional Issues Demonstrate The Lack Of Commonality And Predominance

1. Inclusion Of Users' Personally-Identifiable Information In sWAA-Off Data Is Not An Issue Common To The Class

With respect to injury based on the inadvertent inclusion of users' names, email addresses, and phone numbers in sWAA-off data sets, neither commonality nor predominance is satisfied.

A central contention of Plaintiff Rodriguez's testimony was that his name, email address, and phone number, considered personal information by the parties, were included in sWAA-off data sets provided to Plaintiffs. "My name, my email address, my phone number is all there." Trial Tr. Aug. 25 (Rodriguez) at 826:10. Yet this is not how the collection of sWAA-off data is designed to work. As David Monsees testified, "[W]hen you had WAA off, we would log those logs generated . . . but always to a de-identified ID that happened to be the exact same ID as when you're using Google signed out of your Google Account." Trial Tr. Aug. 20 (Monsees) at 385:4-12. Rather, the inclusion of personally-identifiable information is "extraordinarily rare." Trial Tr. Aug. 29 (Black) at 1712:3-7. Across 132,000 data sets analyzed by Professor Black, only 0.34% included the user's email, and each of these instances was Plaintiff Rodriguez's. *Id.* at 1720:12-15. Indeed, the exemplar data sets admitted as evidence include personally-identifiable information

for only 4 out of the 52 individuals' data that was included. *Id*. at 1712:8-11. Even this is a proportion far higher than what actually occurs. *Id*. at 1712:8-11.

The trial testimony further establishes that this is not a class-wide issue. Plaintiff Rodriguez himself explains, "I mean, ***with me specifically***, it's pretty much you know it's me. My name's in there. . . . [H]ow is it de-identified if my name, my email, my phone number is in there?" Trial Tr. Aug. 25 (Rodriguez) at 826:1-4 (emphasis added). And Plaintiff Santiago never alleged that any of his personal, de-identified information was included in the sWAA-off data sets.

2. Individualized Issues Within The iOS Class

Within the iOS Class (Class 2), there are significant permutations based on differing features of the iOS system over time.

The iOS Class ran from July 1, 2016 to September 23, 2024. Yet, starting in 2021 upon the rollout of iOS 14.5, Apple implemented a feature preventing Google from knowing whether iOS users were Google users. Professor John Black explained, in iOS 14.5, Apple implemented a new policy where iOS users would receive a pop-up notification upon using an app. Trial Tr. Aug. 29 (Black) at 1706:17-23. The pop-up would ask the user: "Ask app not to track." *Id*. at 1706:18-23. If a user enabled this feature, then Google would not be sent a user's device ID (specifically, "IDFA"). *Id*. Without the IDFA, Google would not be able to perform a consent check, and thus could not determine whether an iOS user was a Google user. *Id*. at 1707:4-10.[2] Professor Knittel testified similarly, and added that without a user's IDFA, Google treats the user's data as if the user is "signed out," meaning it is de-identified. Trial Tr. Aug. 28 (Knittel) at 1563:23-1564:8, 1579:21–23.

Based on what iOS Class members understood the iOS 14.5 feature to do, this may impact the analysis as to whether they consented to Google's conduct and whether they had any expectation of privacy over the collection of data. It may be the case that users who disabled the feature, even if they were sWAA-off, thereby consented to the collection of data. Even for those that enabled

[2] If a user allows an app to track, Google is still unable to determine whether a user is sWAA-on or sWAA-off without violating the "core principle" of not mixing pseudonymous data with an identifier. Trial Tr. Aug. 29 (Black) at 1707:11-22.

the feature, users may have understood the "ask app not ***to track***" feature as merely being about identified data, but understood that apps would still *collect* de-identified data. It may even be the case that by "***asking*** app not to track," users were put on notice that apps still *could* track, and thereby collect, data.

This creates further individualized issues, even within just the iOS Class. For example, for every user within the iOS Class, did they start using third-party apps with sWAA off before or after 2021? If after 2021, did they install iOS 14.5? If so, for which apps did they enable the "ask app not to track" feature? Plaintiffs may have to show whether Google was aware that users enabled the "ask app not to track" feature, for which apps, whether this constituted revocation of user consent to collect data, and whether any such consent revocation with respect to the iOS system could be imputed to Google as well.

C. The Court Should Vacate The Jury Verdict On Plaintiffs' Privacy Claims

Plaintiffs' Privacy Claims were tried as a class action. Much of the trial time was focused on issues not specifically related to the class representatives. Plaintiffs' entire damages case, for example, was focused exclusively on the class. The Privacy Claims were tried class-wide, but as demonstrated above, there were no common issues. As a result, the Court should expressly vacate the jury's findings as to the Privacy Claims. *See Spitzfaden v. Dow Corning Corp.*, 833 So.2d 512, 522-23 (La. Ct. App. 2002) (reversing binding effect of verdict on defendant because "status of the case as a class action [at the time of trial] allowed the admission of evidence that would otherwise have had marginal relevance to the case of the eight named plaintiffs" and which was "highly prejudicial" to the defendant); *Bahamas Surgery Ctr. LLC v. Kimberly-Clark Corp.*, 820 F. App'x 563, 566 (9th Cir. 2020) (vacating the judgment as to the defendant because the district court abused its discretion in failing to decertify the class since "the record d[id] not support the conclusion that common questions . . . predominated in the defined class").

IV. CONCLUSION

For the reasons stated above, Google respectfully requests that the Court decertify Plaintiffs' Privacy Claims and vacate the jury verdict as to those claims.

Dated: October 22, 2025

Respectfully submitted,

COOLEY LLP

By: */s/ Jonathan Patchen*

Michael A. Attanasio
Benedict Y. Hur
Simona Agnolucci
Eduardo E. Santacana
Jonathan Patchen
Argemira Flórez
Naiara Toker
Harris Mateen
Thilini Chandrasekera
Isabella McKinley Corbo
Chelsea Hu
Michael B. Morizono

Attorneys for Defendant Google LLC